UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/588,456 | 08/04/2006 | Koichi Ebata | 070639-0149 | 5744 |

22428 7590 11/17/2011

FOLEY AND LARDNER LLP
SUITE 500
3000 K STREET NW
WASHINGTON, DC 20007

| EXAMINER | |
|---|---|
| MAPA, MICHAEL Y | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2617 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 11/17/2011 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/588,456 | EBATA, KOICHI | |
| | Examiner | Art Unit | |
| | MICHAEL MAPA | 2617 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *15 September 2011*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

5)☒ Claim(s) *1-26* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-4,6-10,12-18,20-24 and 26* is/are rejected.

8)☒ Claim(s) *5,11,19 and 25* is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Response to Amendment*

1. The applicant has amended the following:

Claims: 1-2, 5-8, 11-12, 15-17, 21-23 and 25-26 have been amended.

Claims: 3-4, 9-10, 13-14, 18-20 and 24 have not been amended.

### *Response to Arguments*

2. Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 15 and 21 are rejected under 35 U.S.C. 102(e) as being anticipated by Rollins et al. (US Patent Publication 2004/0230671 herein after referenced as Rollins).

Regarding claim 15, Rollins discloses:

A control program embodied on a non-transitory memory that when executed causes a device to perform operations comprising: storing a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

receiving packet transfer information from an access point; detecting a port bound to a wireless interface from said packet transfer information, said wireless interface being the port of the access point, extracting an address of a transfer destination corresponding to said detected port; and estimating that a terminal corresponding to an address registered in a managed terminal list exists as a subordinate of the access point retaining said packet transfer information, wherein said address coincides with said extracted address (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and

compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Regarding claim 21, Rollins discloses:

A monitor method of a wireless network for managing a terminal, comprising: storing a managed terminal list having addresses of terminals registered pre-registered end-user devices, said terminals end-user devices being targets of management where the access point and the end-user devices are separate and independent devices; receiving packet transfer information form an access point; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

detecting a port bound to a wireless interface from said packet transfer information, said wireless interface being the port of the access point; extracting an address of a transfer destination corresponding to said detected port; and estimating that a terminal corresponding to an address registered in said managed terminal list,

said address coinciding with said extracted address, exists as a subordinate of the access point retaining said received packet transfer information (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4, 6-10, 12-14, 16-18, 20, 22-24 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rollins et al. (US Patent Publication 2004/0230671 herein after referenced as Rollins) in view of MacKinnon et al. (US Patent Publication 2004/0177276 herein after referenced as Mackinnon).

Regarding claim 1, Rollins discloses:

A monitor apparatus of a wireless network connected to an access point of the wireless network, said access point retaining packet transfer information including information of a correspondence between a port of said access point and an interface of said port, and information of a correspondence between an address of a transfer destination and the port (Fig. 1 & Fig. 3 & Paragraphs [0030] & [0034]-[0039] of Rollins, wherein Rollins discloses an access point controller (monitoring apparatus) coordinates various operations performed by modular access point and wherein the access controller determines if access to the broadband segment is authorized for the wireless client and if so opening a port in the firewall and updating its internal routing table with the IP address and port number of the requesting client and wherein when a return packet is received from network 128 across the broadband connection, the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table).

said monitor apparatus comprising: a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of

whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

a means configured to receive said packet transfer information from said access point, to detect a port bound to a wireless interface, said wireless interface being the port of the access point, from said packet transfer information, and to extract an address of a transfer destination corresponding to said detected port; and an estimating means for estimating that a terminal corresponding to an address registered in said managed terminal list, said address coinciding with said extracted address, exists as a subordinate of the access point retaining said received packet transfer information (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins discloses the access point controller to be part of the access point. However, Rollins fails to disclose "a monitor apparatus of a wireless network connected to an access point of the wireless network via a network."

In a related field of endeavor, Mackinnon discloses:

a monitor apparatus of a wireless network connected to an access point of the wireless network via a network; said monitor apparatus comprising: a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user

has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller). Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication as well as providing the system with a way to centralize the authentication process of multiple access points / control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 2, Rollins discloses:

A monitor apparatus of a wireless network connected to an access point of wireless network (Fig. 1 & Fig. 3 & Paragraphs [0030] & [0034]-[0039] of Rollins, wherein Rollins discloses an access point controller (monitoring apparatus) coordinates

various operations performed by modular access point and wherein the access controller determines if access to the broadband segment is authorized for the wireless client and if so opening a port in the firewall and updating its internal routing table with the IP address and port number of the requesting client and wherein when a return packet is received from network 128 across the broadband connection, the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table).

said monitor apparatus comprising: a managed terminal list having addresses of terminals pre-registered end- user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

a means configured to receive said packet transfer information from said access point, to detect a port bound to a wireless interface, said wireless interface being the port of the access point, from said packet transfer information, and to extract an address of a transfer destination corresponding to said detected port; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point

controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins discloses the access point controller to be part of the access point. However, Rollins fails to disclose "a monitor apparatus of a wireless network connected to an access point of wireless network via a network," and "a determining means for investigating an operation situation of a terminal corresponding to an address registered in said managed list, said list address coinciding with said extracted address, to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation."

In a related field of endeavor, Mackinnon discloses:

a monitor apparatus of a wireless network connected to an access point of wireless network via a network, said monitor apparatus comprising: a managed terminal list having addresses of terminals pre-registered end- user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access

point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

a determining means for investigating an operation situation of a terminal corresponding to an address registered in said managed list, said list address coinciding with said extracted address, to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation (Fig. 1 & Fig. 5 & Paragraphs [0074] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the

IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system, therefore the authentication and control program which provides authentication and provisioning can be implemented in the backend authentication system separate from the control device).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller) and wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can

determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system. Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device and which checks the status of a user's session using port scans and ARP pings and removes the control session from the list of active sessions in the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication and provisioning as well as monitoring for active sessions as well as providing the system with a way to centralize the authentication process of multiple access points / control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 3, Rollins in view of Mackinnon discloses:

The monitor apparatus of a wireless network according to claim 2, further comprising: a determining means for comparing said extracted address with an address

described in said managed terminal list, and for, in a case where said extracted address is not included in said managed terminal list, determining that an access to the access point retaining said packet transfer information has been made by a terminal that is not a target of management (Fig. 3 & Paragraphs [0037]-[0038] of Rollins & Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Rollins discloses determining if the client is authorized before opening a port in the firewall and updating the routing table and wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

Regarding claim 4, Rollins in view of Mackinnon discloses:

The monitor apparatus of a wireless network according to claim 2 (see claim 2 further comprising: a means for drawing a result on a relation between an access point and terminals, which are estimated to be existent as subordinates of said access point, or are determined to be in connection with said access point, for all the access points under management thereof to display a relation between each access point and each

terminal that is estimated to be existent as a subordinate of each access point, or each terminal that is determined to be in connection with each access point (Paragraphs [0091]-[0093] of Mackinnon, wherein Mackinnon discloses the user physically roaming a wired or wireless environment wherein a control device can solicit feedback from any federation of control devices with which it has joined to determine if this particular user has an active session and should be granted a new session without the requirement to authenticate and the new control device can dynamically remap the network connections and configuration of a roaming user's user device in the event that the new control device is configured differently or controls a different subnet wherein the new control device can remap the IP address of the user device according to any IP mapping scheme known in the art. Roaming and handover are a commonly known characteristic and event of a wireless network wherein it is commonly known in the art that the handover registration can be implemented by either the mobile device or the network. In addition, soft-handover is also commonly known in the art wherein a mobile device is simultaneously connected with both the new base station and the previous base station before the previous base station connection is disconnected. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins in view of Mackinnon to incorporate the teachings of Mackinnon for the purpose of improving the system by providing the system with a way to handle roaming situations).

Regarding claim 6, Rollins in view of Mackinnon discloses:

The monitor apparatus of a wireless network according to claim 2, wherein, in a case where the address of the identical terminal has been described in said packet transfer information retained by plural access points, including: a means for, from said terminal, acquiring identification information of the wireless network to which said terminal belongs; a means for comparing identification information of said plural access points with the identification information acquired from said terminal; and a means for estimating that said terminal exists as a subordinate of the access point having the identification information identical to the identification information acquired from said terminal, or determining that said terminal has a connection with its access point (Paragraphs [0091]-[0093] of Mackinnon, wherein Mackinnon discloses the user physically roaming a wired or wireless environment wherein a control device can solicit feedback from any federation of control devices with which it has joined to determine if this particular user has an active session and should be granted a new session without the requirement to authenticate and the new control device can dynamically remap the network connections and configuration of a roaming user's user device in the event that the new control device is configured differently or controls a different subnet wherein the new control device can remap the IP address of the user device according to any IP mapping scheme known in the art. Roaming and handover are a commonly known characteristic and event of a wireless network wherein it is commonly known in the art that the handover registration can be implemented by either the mobile device or the network. In addition, soft-handover is also commonly known in the art wherein a mobile device is simultaneously connected with both the new base station and the previous

base station before the previous base station connection is disconnected. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins in view of Mackinnon to incorporate the teachings of Mackinnon for the purpose of improving the system by providing the system with a way to handle roaming situations).

Regarding claim 7, Rollins discloses:

A monitor system of a wireless network, said monitor system comprising: at least one access point of a wireless network, said at least one access point retaining packet transfer information including information of a correspondence between a port of said at least one access point and an interface of said port, and information of a correspondence between an address of a transfer destination and the port; at least one terminal of the wireless network; and a monitor apparatus connected to said at least one access point, (Fig. 1 & Fig. 3 & Paragraphs [0030] & [0034]-[0039] of Rollins, wherein Rollins discloses an access point controller (monitoring apparatus) coordinates various operations performed by modular access point and wherein the access controller determines if access to the broadband segment is authorized for the wireless client and if so opening a port in the firewall and updating its internal routing table with the IP address and port number of the requesting client and wherein when a return packet is received from network 128 across the broadband connection, the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table).

wherein said monitor apparatus comprises: a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

a means configured to receive said packet transfer information from said at least one access point, to detect a port bound to a wireless interface, said wireless interface being the port of the at least one access point, from said packet transfer information, and to extract an address of a transfer destination corresponding to said detected port; and an estimating means for estimating that a terminal corresponding to an address registered in said managed terminal list, said address coinciding with said extracted address, exists as a subordinate of the access point retaining said received packet transfer information (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found,

the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins discloses the access point controller to be part of the access point. However, Rollins fails to disclose "a monitor apparatus connected to said at least one access point via a network."

In a related field of endeavor, Mackinnon discloses:

a monitor apparatus connected to said at least one access point via a network, wherein said monitor apparatus comprises: a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the

control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller). Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication

as well as providing the system with a way to centralize the authentication process of multiple access points / control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 8, Rollins discloses:

A monitor system of a wireless network, said monitor system comprising: at least one access point of the wireless network; at least one terminal of the wireless network; and a monitor apparatus connected to said access point, (Fig. 1 & Fig. 3 & Paragraphs [0030] & [0034]-[0039] of Rollins, wherein Rollins discloses an access point controller (monitoring apparatus) coordinates various operations performed by modular access point and wherein the access controller determines if access to the broadband segment is authorized for the wireless client and if so opening a port in the firewall and updating its internal routing table with the IP address and port number of the requesting client and wherein when a return packet is received from network 128 across the broadband connection, the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table).

wherein said monitor apparatus comprises: a managed terminal list having addresses of terminals registered pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate

devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

a means configured to receive said packet transfer information from said at least one access point, to detect a port bound to a wireless interface, said interface being the port of the at least one access point, from said packet transfer information, and to extract an address of a transfer destination corresponding to said detected port; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins discloses the access point controller to be part of the access point. However, Rollins fails to disclose "a monitor apparatus connected to said access point via a network" and "a determining means for investigating an operation situation of a

terminal corresponding to an address registered in said managed list, said list address coinciding with said extracted address, to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation."

In a related field of endeavor, Mackinnon discloses:

a monitor apparatus connected to said access point via a network, wherein said monitor apparatus comprises: a managed terminal list having addresses of terminals registered pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

a determining means for investigating an operation situation of a terminal corresponding to an address registered in said managed list, said list address coinciding

with said extracted address, to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation (Fig. 1 & Fig. 5 & Paragraphs [0074] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system, therefore the authentication and control program which provides authentication and provisioning can be implemented in the backend authentication system separate from the control device).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user

has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller) and wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system. Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device and

which checks the status of a user's session using port scans and ARP pings and removes the control session from the list of active sessions in the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication and provisioning as well as monitoring for active sessions as well as providing the system with a way to centralize the authentication process of multiple access points / control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 9, Rollins in view of Mackinnon discloses "The monitor system of a wireless network according to claim 8." The examiner rejects claim 9 with the same arguments provided above (see claim 3).

Regarding claim 10, Rollins in view of Mackinnon discloses "The monitor system of a wireless network according to claim 8." The examiner rejects claim 10 with the same arguments provided above (see claim 4).

Regarding claim 12, Rollins in view of Mackinnon discloses "The monitor system of a wireless network according to claim 8." The examiner rejects claim 12 with the same arguments provided above (see claim 6).

Regarding claim 13, Rollins in view of Mackinnon discloses:

The monitor system of a wireless network according to claim 8, wherein: said terminal includes a means for transmitting a broadcast packet; and said access point includes a means for updating the packet transfer information that the access point retains based upon said broadcast packet (Figs. 2-3 & Paragraphs [0034]-[0038] of

Rollins & Paragraphs [0034]-[0040] of Mackinnon, wherein Rollins discloses the access point receiving a packet from the client and upon authorization updating the routing table with the IP address and port number of the requesting client and wherein Mackinnon discloses the user sending network communication and the control device monitoring network for network communications and authenticating the user and upon successful authentication receiving user profile information and establishing provisioning rules based on the user profile. In addition, the examiner takes official notice that it is commonly known in the art for the terminal / end user device / mobile stations to be able to broadcast packets to access points).

Regarding claim 14, Rollins in view of Mackinnon discloses:

The monitor system of a wireless network according to claim 8, wherein said access point further comprises: a means for notifying to the other access point information as to which access point to which the terminal belongs; and a means for updating the packet transfer information that the access point retains based upon said information as to which access point to which said terminal belongs (Paragraphs [0091]-[0093] of Mackinnon, wherein Mackinnon discloses the user physically roaming a wired or wireless environment wherein a control device can solicit feedback from any federation of control devices with which it has joined to determine if this particular user has an active session and should be granted a new session without the requirement to authenticate and the new control device can dynamically remap the network connections and configuration of a roaming user's user device in the event that the new control device is configured differently or controls a different subnet wherein the new

control device can remap the IP address of the user device according to any IP mapping scheme known in the art. Roaming and handover are a commonly known characteristic and event of a wireless network wherein it is commonly known in the art that the handover registration can be implemented by either the mobile device or the network. In addition, soft-handover is also commonly known in the art wherein a mobile device is simultaneously connected with both the new base station and the previous base station before the previous base station connection is disconnected. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins in view of Mackinnon to incorporate the teachings of Mackinnon for the purpose of improving the system by providing the system with a way to handle roaming situations).

Regarding claim 16, Rollins discloses:

A control program embodied on a non-transitory memory that when executed causes a device to perform operations comprising: storing a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an

authorization record for the wireless client has already been registered prior to the check).

receiving packet transfer information from an access point; detecting a port bound to a wireless interface from said packet transfer information, said wireless interface being the port of the access point; extracting an address of a transfer destination corresponding to said detected port; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins fails to disclose "and investigating an operation situation of a terminal corresponding to an address registered in a managed list to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation, wherein said address coincides with said extracted address."

In a related field of endeavor, Mackinnon discloses:

storing a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management, where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

and investigating an operation situation of a terminal corresponding to an address registered in a managed list to determine that said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation, wherein said address coincides with said extracted address (Fig. 1 & Fig. 5 & Paragraphs [0074] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for

session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system, therefore the authentication and control program which provides authentication and provisioning can be implemented in the backend authentication system separate from the control device).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the

control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller) and wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system. Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device and which checks the status of a user's session using port scans and ARP pings and removes the control session from the list of active sessions in the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication and provisioning as well as monitoring for active sessions as well as providing the system with a way to centralize the authentication process of multiple access points /

control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 17, Rollins in view of Mackinnon discloses "The control program according to claim 16." The apparatus claims disclosed above performs the functionalities that correspond to the control program claim, therefore the examiner rejects claim 17 with the same arguments provided above (see claim 3).

Regarding claim 18, Rollins in view of Mackinnon discloses "The control program according to claim 16." The apparatus claims disclosed above performs the functionalities that correspond to the computer program product claim, therefore the examiner rejects claim 18 with the same arguments provided above (see claim 4).

Regarding claim 20, Rollins in view of Mackinnon discloses " The control program according to claim 16" The apparatus claims disclosed above performs the functionalities that correspond to the computer program product claim, therefore the examiner rejects claim 20 with the same arguments provided above (see claim 6).

Regarding claim 22, Rollins discloses:

A monitor method of a wireless network for managing a terminal, comprising: storing a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management where the access point and the end-user devices are separate and independent devices; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses the wireless client and the access point as separate devices and wherein the access to the broadband segment is determined to be authorized or not for the wireless client, therefore the

wireless client are pre-registered since the check of whether the wireless client is authorized or not would indicate that an authorization record for the wireless client has already been registered prior to the check).

receiving packet transfer information form an access point; detecting a port bound to a wireless interface from said packet transfer information, said wireless interface being the port of the access point; extracting an address of a transfer destination corresponding to said detected port; (Fig. 1 & Fig. 3 & Paragraphs [0037]-[0039] of Rollins, wherein Rollins discloses receiving a return packet from the network 128 and the access point firewall routes the packet to the access point controller wherein the access point controller examines the packet header and compares the IP address and port number with IP addresses and port numbers in its internal routing table and if a match is found, the packet is passed to the appropriate client on the wireless segment and if the IP address and the port number are not found in the internal routing table of access point controller then the packet is dropped by access point controller, therefore if the address is located within the internal routing table then it is an indication that the wireless client is a subordinate of the access point).

Rollins fails to disclose "and investigating an operation situation of a terminal corresponding to an address registered in said managed list, said list addresses coinciding with said extracted address, to determine if said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation."

In a related field of endeavor, Mackinnon discloses:

storing a managed terminal list having addresses of terminals pre-registered end-user devices, said end-user devices being targets of management where the access point and the end-user devices are separate and independent devices; receiving packet transfer information form an access point; (Fig. 1 & Paragraphs [0035]-[0037], [0042] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials such as the MAC address and IP address in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller)).

and investigating an operation situation of a terminal corresponding to an address registered in said managed list, said list addresses coinciding with said extracted address, to determine if said terminal having said extracted address has a connection with the access point retaining said received packet transfer information in a case where said terminal having said address is in operation (Fig. 1 & Fig. 5 & Paragraphs [0074] & [0046]-[0047] of Mackinnon, wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for

session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system, therefore the authentication and control program which provides authentication and provisioning can be implemented in the backend authentication system separate from the control device).

Rollins discloses an access point comprising an access point controller which determines whether access is authorized for the wireless client or not and discloses examining the received packet and comparing the IP address and port number with IP address and port numbers in its internal routing table and if a match is found the packet is passed to the appropriate client and if not the packet is dropped. Mackinnon discloses a control device (access point) receiving IP packets can determine if a user has been authenticated and if not the control device can receive the user credentials and send the credentials to authentication system 22 wherein the system can compare the credentials in authentication database to determine if user is permitted to access the network and wherein Mackinnon discloses the control device can authenticate the user by initiating a comparison between the received credentials and the credentials for authorized users wherein the authentication can be done at the control device or the

control device can authenticate the user by sending the credentials to a backend authentication system (monitoring apparatus / access point controller) and wherein Mackinnon discloses in addition to authentication and provisioning, authentication and control program 61 can provide session monitoring wherein session monitor can monitor a control session for session characteristics such as a session time out and can determine if a user's session is still active by for example performing port scans and ARP pings and if the session monitor determines that a control session is timed out, session monitor can remove the control sessions from the list of active sessions returning the user to an unauthenticated state and delete the user specific rules for the associated user from the IP table and wherein Mackinnon discloses the authentication can be performed at the control device or the control device can authenticate the user by sending the credentials to a backend authentication system. Different functionalities embodied in multiple separate devices or in one single device is a commonly known concept in the art. Therefore, it would have been obvious to one of ordinary skill in the art to modify the invention of Rollins to incorporate the teachings of Mackinnon of having an authentication system separate from the access point / control device and which checks the status of a user's session using port scans and ARP pings and removes the control session from the list of active sessions in the access point / control device for the purpose of improving the system by reducing the processing load within the access point / control device in having a separate device perform the authentication and provisioning as well as monitoring for active sessions as well as providing the system with a way to centralize the authentication process of multiple access points /

control devices to a specific remote and separate authentication device as well as improving the system by conforming to commonly known teachings in the art.

Regarding claim 23, Rollins in view of Mackinnon discloses "The monitor method of a wireless network according to claim 22." The examiner rejects claim 23 with the same arguments provided above (see claim 3).

Regarding claim 24, Rollins in view of Mackinnon discloses "The monitor method of a wireless network according to claim 22." The examiner rejects claim 24 with the same arguments provided above (see claim 4).

Regarding claim 26, Rollins in view of Mackinnon discloses " The monitor method of a wireless network according to claim 22." The examiner rejects claim 26 with the same arguments provided above (see claim 6).

***Allowable Subject Matter***

7. Claims 5, 11, 19 and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

***Conclusion***

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL MAPA whose telephone number is (571)270-5540. The examiner can normally be reached on MONDAY TO THURSDAY 8:00AM - 5:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Dwayne Bost can be reached on (571)272-7023. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Michael Mapa/
Examiner, Art Unit 2617

/Erika A. Gary/
Primary Examiner, Art Unit 2617